AMENDMENTS TO CLAIMS

1. (currently amended): A system comprising a plurality of client computers, a server separate from the plurality of client computers, and a plurality of computer readable media, wherein

each computer readable medium within said ~~plucality~~ plurality of computer readable media is transportable to each client computer in said plurality of client computers and is readable and writable within each client computer in said plurality of client computers,

said server generates a secure transfer key pair and encrypts a private key of said secure transfer key pair,

said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form, and

each client computer in said plurality thereof is programmed to generate token data including said portion of said token data encrypted with a public key of said secure transfer key pair, to record said token data on a computer readable medium in said plurality of computer readable media, to read said token data from a computer readable medium in said plurality of computer readable media, to decrypt said private key of said secure transfer key pair, to decrypt said portion of said token data with said private key of said secure transfer key pair, and to be enabled to perform a predetermined task after decrypting said portion of said token data.

2. (previously presented): The system of claim 1, wherein

each client computer in said plurality thereof generates a platform key pair,

a public key of said platform key pair is transferred to said server, and

said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer

key pair encrypted with said public key of said platform key pair of said client computer, and each client computer in said plurality thereof stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair.

3. (original): The system of claim 2, wherein

each client computer in said plurality thereof includes a security subsystem having a subsystem processor and subsystem storage,

each client computer in said plurality thereof generates a hardware key pair within said security subsystem

a private key of said hardware key pair is stored in said subsystem storage, and

a private key of said platform key pair is encrypted with said hardware public key and is decrypted with said hardware private key in said security subsystem before said private key of said platform key pair is used to decrypt said private key of said secure transfer key pair within said security subsystem.

4. (canceled)

5. (original): The system of claim 1, wherein

each client computer in said plurality of client computers includes an input device for providing a numeric input,

said portion of said token data includes a PIN,

each client computer in said plurality of client computers, after decrypting said portion of said token data read from said computer readable medium, compares said PIN included within said token data with said numeric input provided through said input device, and

each client computer within said plurality of client computers is enabled

to perform a predetermined task in response to determining an equivalence between said PIN and said numeric input provided through said input device.

6. (original) The system of claim 1, wherein

said system additionally comprises a communications network connecting said server with each of said client computers in said plurality thereof, and

said secure transfer key is transmitted over said communications network from said server to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in said encrypted form.

7. (original) The system of claim 6, wherein

each client computer in said plurality thereof generates a platform key pair and transmits a public key of said platform key pair to said server over said communications network,

said server transmits said secure transfer key pair over said communications network to each of said client computers in said plurality thereof with said platform key pair of said client computer, and

each client computer in said plurality thereof stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair.

8. (original) The system of claim 1, wherein

said server writes said secure transfer key pair on a computer readable medium with said private key of said secure transfer key pair in said encrypted form, and

each of said client computers in said plurality thereof reads said secure transfer key pair with said private key of said secure transfer key pair in said encrypted form from said computer readable medium.

9. (previously presented): The system of claim 8, wherein

each client computer in said plurality thereof generates a platform key pair and writes a public key of said platform key pair on a first computer readable medium,

said server reads said public key of said platform key pair from each client computer in said plurality thereof , encrypts said private key of said secure transfer key pair with said public key of said platform key pair, and writes said secure transfer key pair on a second computer readable medium with said private key of said secure transfer key pair encrypted with said public key of said client computer, and

said client computer reads said secure transfer key pair with said private key so said secure transfer key pair encrypted with said public key of said client computer from said second computer readable medium, stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair.

10. (currently amended): A method within a ~~computing~~ client computer system within a plurality of client computer systems for generating a token causing ~~a~~ another computer system in ~~a~~ the plurality of computer systems to be enabled to perform a predetermined task and for reading a token to be enabled to perform a predetermined task, wherein said method comprises:

receiving a secure transfer key pair generated within a server separate from said plurality of computer systems;

storing said secure transfer key pair;

after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair; and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium;

after storing said secure transfer key pair, in response to an indication that token data is to be read, reading said token data from a computer readable medium, and decrypting a portion of said data with a private key of said secure transfer key pair.

11. (original): The method of claim 10, wherein said secure transfer key pair is received from said server over a communications network.

12. (original): The method of claim 11, additionally comprising:

generating and storing a platform key pair;

transmitting a public key of said platform key pair to said server over said communications network, wherein said secure transfer key pair is subsequently received from said server encrypted with said public key of said platform key pair, and wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

13. (original): The method of claim 10, wherein said secure transfer key pair is read from a computer readable medium.

14. (previously presented): The method of claim 13, additionally comprising:

generating and storing a platform key pair;

writing a public key of said platform key pair on a computer readable medium;

reading said secure transfer key pair from a computer readable medium encrypted with said public key of said platform key pair, wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair; and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

15. (original): The method of claim 10, additionally comprising:

generating and storing a hardware key pair within a security subsystem of said computing system, wherein a private key of said hardware key pair is stored within said security subsystem of said computing system;

encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and

decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

16. (original): The method of claim 10, additionally comprising enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

17. (original): The method of claim 10, wherein

said portion of said token data includes a PIN, and

said method additionally comprises receiving a numeric input from an

input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

18. (currently amended): A computer readable medium having recorded thereon computer executable instructions for performing a method within a ~~computing~~ client computer system within a plurality of client computer systems for generating a token causing ~~a~~ another computer system in ~~a~~ the plurality of computer systems to be ~~eneabled~~ enabled to perform a predetermined task and for reading a token to be enabled to perform a predetermined task, wherein said method comprises:

receiving a secure transfer key pair from a server separate from said plurality of computer systems;

storing said secure transfer key pair;

after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium;

after storing said secure transfer key pair, in response to an indication that token data is to be read, reading said token data from a computer readable medium, and decrypting a portion of said data with a private key of said secure transfer key pair, and

being enabled to perform a predetermined task after decrypting said portion of said data.

19. (original): The computer readable medium of claim 18, wherein said secure transfer key pair is received from said server over a communications network.

20. (original): The computer readable medium of claim 19, wherein said method additionally comprises:

generating and storing a platform key pair;

transmitting a public key of said platform key pair to said server over said communications network, wherein said secure transfer key pair is subsequently received from said server encrypted with said public key of said platform key pair, and wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

21. (original): The computer readable medium of claim 18, wherein said secure transfer key pair is read from a computer readable medium.

22. (previously presented): The computer readable medium of claim 21, wherein said method additionally comprises:

generating and storing a platform key pair;

writing a public key of said platform key pair on a computer readable medium;

reading said secure transfer key pair from a computer readable medium encrypted with said public key of said platform key pair, wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair; and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

23. (original): The computer readable medium of claim 18, wherein said method additionally comprises:

generating and storing a hardware key pair within a security subsystem of said computing system, wherein a private key of said hardware key pair is stored within said security subsystem of said computing system;

encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and

decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

24. (original): The computer readable medium of claim 18, wherein said method additionally comprises enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

25. (original): The computer readable medium of claim 18, wherein:

said portion of said token data includes a PIN, and

said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

26. (currently amended): A process of providing electrical signals over a communications network causing computer storage to have stored therein computer executable instructions for performing a method within a ~~computing~~ client computer system in a plurality of computer systems for encrypting token

data, for generating a token causing ~~a~~ another computer system in ~~a~~ the plurality of computer systems to be enabled to perform a predetermined task and for reading a token to be enabled to perform a predetermined task, wherein said method comprises:

receiving a secure transfer key pair from a server separate from said computer system;

storing said secure transfer key pair;

after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair~~;~~ and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium;

after storing said secure transfer key pair, in response to an indication that token data is to be read, reading said token data from a computer readable medium, and decrypting a portion of said data with a private key of said secure transfer key pair, and

being enabled to perform a predetermined task after decrypting said portion of said data.

27. (original): The process of claim 26, wherein said secure transfer key pair is received from said server over a communications network.

28. (original): The process of claim 27, wherein said method additionally comprises:

generating and storing a platform key pair;

transmitting a public key of said platform key pair to said server over said communications network, wherein said secure transfer key pair is subsequently received from said server encrypted with said public key of said platform key pair, and wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

29. (original): The process of claim 26, wherein said secure transfer key pair is read from a computer readable medium.

30. (previously presented): The process of claim 29, additionally comprising:
generating and storing a platform key pair;
writing a public key of said platform key pair on a computer readable medium,
reading said secure transfer key pair from a computer readable medium encrypted with said public key of said platform key pair, wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and
decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

31. (original): The process of claim 26, wherein said method additionally comprises:
generating and storing a hardware key pair within a security subsystem of said computing system, wherein a private key of said hardware key pair is stored within said security subsystem of said computing system;
encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key pair; and
decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform

key pair.

32. (original): The process of claim 26, wherein said method additionally comprises enabling performance of a predetermined task in response to decrypting said portion of said data with said private key of said secure transfer key pair.

33. (original): The process of claim 26, wherein:

said portion of said token data includes a PIN, and

said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

34. (currently amended): A method for enabling performance of predetermined tasks in a local computer and in a remote computer system through use of an encrypted portion of token data recorded in the local computer, wherein said method comprises:

generating a secure transfer key pair within a server separate from said local computer and from said remote computer;

transferring said secure transfer key pair from said server to said local computer;

storing said secure transfer key pair within said local computer;

establishing communication between said remote computer and said server;

transferring said secure transfer key pair from said server to said remote computer;

storing said secure transfer key pair within said remote computer;

encrypting said portion of said token data within said local computer with a public key of said secure transfer key pair;

recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said local computer on a computer readable medium;

reading said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said secure transfer key pair, within said remote computer from said computer readable medium;

decrypting said portion of said ~~gtoken~~ token data within said local computer with a private key of said secure transfer key pair;

enabling said performance of a predetermined task within said local computer in response to decrypting said portion of said token data;

transporting said computer readable medium from said local computer to said remote computer; reading said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair, within said remote computer from a said computer readable medium;

decrypting said portion of said token data within said remote computer with a private key of said secure transfer key pair; and

enabling said performance of a predetermined task in said remote computer in response to decrypting said portion of said token data.

35. (previously presented): The method of claim 34, wherein said secure transfer key pair is received from said server over a communications network.

36. (original): The method of claim 34, additionally comprising:

generating and storing a first platform key pair within said local computer; and

transmitting a public key of said first platform key pair to said server from said local computer, wherein said secure transfer key pair is subsequently received by said local computer from said server encrypted with said public key of said first platform key pair, and wherein said private key of said secure transfer

key pair is stored within said local computer encrypted with said public key of said first platform key pair.

37. (original): The method of claim 34, wherein said secure transfer key pair is read from a computer readable medium.

38. (original): The method of claim 37, wherein said method additionally comprises:

generating and storing a platform key pair;

writing a public key of said platform key pair on a computer readable medium,

reading said secure transfer key pair from a computer readable medium encrypted with said public key of said platform key pair, and wherein said private key of said secure transfer key pair is stored encrypted with said public key of said platform key pair, and

decrypting said private key of said secure transfer key pair with said private key of said platform key pair before decrypting said portion of said data with said private key of said secure transfer key pair.

39. (original): The method of claim 34, additionally comprising:

generating and storing a first hardware key pair in a security subsystem of said local computer, wherein a private key of said hardware key pair is stored within said security subsystem of said local computer;

encrypting said private key of said first platform key pair with said public key of said first hardware key pair within said local computer, wherein said first platform key pair is stored within said local computer with said private key of said first platform key pair encrypted with said public key of said first hardware key pair.

40. (original): The method of claim 34, additionally comprising:

generating and storing a second platform key pair within said remote computer;

transmitting a public key of said second platform key pair to said server from said remote computer, wherein said secure transfer key pair is subsequently received by said remote computer from said server encrypted with said public key of said second platform key pair, and wherein said private key of said secure transfer key pair is stored within said remote computer encrypted with said public key of said second platform key pair, and

decrypting said private key of said secure transfer key pair with said private key of said second platform key pair within said remote computer before decrypting said portion of said data with said private key of said secure transfer key pair.

41. (original): The method of claim 34, additionally comprising:

generating and storing a second hardware key pair within a security subsystem of said remove computer, wherein a private key of said hardware key pair is stored within said security subsystem of said remote computer;

encrypting said private key of said second platform key pair with said public key of said second hardware key pair within said remote computer, wherein said second platform key pair is stored within said remote computer with said private key of said second platform key pair encrypted with said public key of said second hardware key pair; and

decrypting said private key of said second platform key pair with said private key of said second hardware key pair within said security subsystem of said remote computer before decrypting said private key of said secure transfer key pair with said private key of said second platform key pair.

42. (canceled)

43. (original): The method of claim 36, wherein

said portion of said token data encrypted with said public key of said secure transfer key pair includes a PIN, and

said method additionally comprises receiving a numeric input within said remote computer from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task within said remote computer in response to determining an equivalence between said PIN and said numeric input.

44. (previously presented): A method for establishing a plurality of associated client computers, wherein a client computer in said plurality of associated client computers performs a predetermined task in response to reading and decrypting token data recorded on a computer readable medium, wherein said method comprises:

generating a secure transfer key pair within a server separate from said plurality of associated client computers;

transferring said secure transfer key pair from said server to each client computer in said plurality of associated client computers;

storing said secure transfer key pair within each client computer in said plurality of associated client computers;

encrypting a first portion of token data with a public key of said secure transfer key pair within a first client computer within said plurality of associated client computers;

recording token data on a computer readable medium, wherein said token data includes said first portion of token data encrypted with said public key of said secure transfer key pair, in said first client computer;

transferring said computer readable medium from said first client computer to a second client computer within said plurality of associated client computers; reading said token data on said second client computer; and

decrypting said token data encrypted with said public key of said secure transfer key pair with a private key of said secure transfer key pair in said second client computer.

45. (original): The method of claim 44, wherein

each client computer within said plurality of associated client computers generates a platform key pair,

a public key of said platform key pair is transferred from said client computer to said server,

said private key of said secure transfer key pair is encrypted within said server with said public key of said platform key pair,

said secure transfer key pair is transferred from said server to said client computer with a private key of said secure transfer key pair encrypted with said public key of said platform key pair.

46. (original): The method of claim 45, wherein said secure transfer key pair is transferred from said server to said client computer on a computer readable medium.

47. (original): The method of claim 45, wherein said secure transfer key pair is transferred from said server to said client computer by transmission over a communications network.

48. (original): The method of claim 45, additionally comprising:

generating and storing a hardware key pair within a security subsystem of said client system, wherein a private key of said hardware key pair is stored within said security subsystem of said client computer;

encrypting said private key of said platform key pair with said public key of said hardware key pair, wherein said platform key pair is stored with said private key of said platform key pair encrypted with said public key of said hardware key

pair; and

decrypting said private key of said platform key pair with said private key of said hardware key pair within said security subsystem before decrypting said private key of said secure transfer key pair with said private key of said platform key pair.

49. (original): The method of claim ~~10~~ 45, wherein

a portion of said token data includes a PIN, and

said method additionally comprises receiving a numeric input from an input device, comparing said PIN with said numeric input from said input device, and enabling performance of a predetermined task in response to determining an equivalence between said PIN and said numeric input.

50. (previously presented): A method for establishing a plurality of associated client computers, wherein a client computer in said plurality of associated client computers performs a predetermined task in response to reading and decrypting token data recorded on a computer readable medium, wherein said method comprises:

generating a secure transfer key pair within a server separate from said plurality of associated client computers;

transferring said secure transfer key pair from said server to each client computer in said plurality of associated client computers; and

storing said secure transfer key pair within each client computer in said plurality of associated client computers.

51. (original): The method of claim 50, wherein

said method additionally comprises receiving a platform key pair from said client computer within said plurality of associated client computers before transferring said secure transfer key pair to said client computer,

said secure transfer key pair is transferred from said server to said client

computer with a private key of said secure transfer key pair encrypted with said public key of said platform key pair.

52. (original): The method of claim 51, wherein said secure transfer key pair is transferred from said server to said client computer over a communications network.

53. (original): The method of claim 51, wherein said secure transfer key pair is transferred from said server to said client computer as data recorded on a computer readable medium.